

# POWER SUMS OVER FINITE COMMUTATIVE UNITAL RINGS

JOSÉ MARÍA GRAU AND ANTONIO M. OLLER-MARCÉN

**ABSTRACT.** In this paper we compute the sum of the  $k$ -th powers over any finite commutative unital rings, thus generalizing known results for finite fields, the rings of integers modulo  $n$  or the ring of Gaussian integers modulo  $n$ . As an application we focus on quotient rings of the form  $\mathbb{Z}/n\mathbb{Z}[x]/(f(x))$  for any polynomial  $f \in \mathbb{Z}[x]$ .

AMS 2010 Mathematics Subject Classification 13B99, 13A99, 13F99

Keywords: Power sum, Finite commutative unital ring, Polynomial ring over  $\mathbb{Z}/n\mathbb{Z}$

## 1. INTRODUCTION

For a finite ring  $R$  and  $k \geq 1$ , we define the power sum

$$S_k(R) := \sum_{r \in R} r^k.$$

Throughout the paper we will deal only with finite commutative unital rings and our main objective will be the computation of  $S_k(R)$  in such case.

The problem of computing  $S_k(R)$  is completely solved only for some particular families of finite rings. If  $R$  is a finite field  $\mathbb{F}_q$ , the value of  $S_k(\mathbb{F}_q)$  is well-known. If  $R = \mathbb{Z}/n\mathbb{Z}$ , the study of  $S_k(\mathbb{Z}/n\mathbb{Z})$  dates back to 1840 [10] and has been completed in various works [2, 6, 9]. More recently, the case  $R = \mathbb{Z}/n\mathbb{Z}[i]$  has been solved in [3]. In these cases, we have the following results.

**Proposition 1.** *Let  $k \geq 1$  be an integer.*

i) *Finite fields:*

$$S_k(\mathbb{F}_q) = \begin{cases} -1, & \text{if } (q-1) \mid k; \\ 0, & \text{otherwise.} \end{cases}$$

ii) *Integers modulo  $n$ :*

$$S_k(\mathbb{Z}/n\mathbb{Z}) = \begin{cases} -\sum_{p \mid n, p-1 \mid k} \frac{n}{p}, & \text{if } k \text{ is even or } k=1 \text{ or } n \not\equiv 0 \pmod{4}; \\ 0, & \text{otherwise.} \end{cases}$$

iii) *Gaussian integers modulo  $n$ :*

$$S_k(\mathbb{Z}/n\mathbb{Z}[i]) = \begin{cases} \frac{n}{2}(1+i), & \text{if } k > 1 \text{ is odd and } n \equiv 2 \pmod{4}; \\ -\sum_{p \in \mathcal{P}(k,n)} \frac{n^2}{p^2}, & \text{otherwise.} \end{cases}$$

where

$$\mathcal{P}(k, n) := \{\text{prime } p : p \mid n, p^2 - 1 \mid k, p \equiv 3 \pmod{4}\}$$

and  $p \parallel n$  means that  $p \mid n$ , but  $p^2 \nmid n$ .

On the other hand, there are not many works dealing with the non-commutative case. The case of square matrices over finite fields is studied in [1], where the following result is proved.

**Proposition 2.** *Let  $k, d \geq 1$  be integers. Then  $S_k(\mathbb{M}_d(\mathbb{F}_q)) = 0$  unless  $q = 2 = d$  and  $1 < k \equiv -1, 0, 1 \pmod{6}$  in which case  $S_k(\mathbb{M}_d(\mathbb{F}_q)) = I_2$ .*

In [4] some general results for  $S_k(\mathbb{M}_d(\mathbb{Z}/n\mathbb{Z}))$  are proved and the following conjecture is made about power sums of matrix rings over finite commutative rings.

**Conjecture 1.** *Let  $d > 1$  and let  $R$  be a finite commutative ring. Then,  $S_k(\mathbb{M}_d(R)) = 0$  unless the following conditions hold:*

- i)  $d = 2$ ,
- ii)  $|R| \equiv 2 \pmod{4}$  and  $1 < k \equiv -1, 0, 1 \pmod{6}$ ,
- iii) *The unique element  $e \in R \setminus \{0\}$  such that  $2e = 0$  is idempotent.*

Moreover, in this case

$$S_k(\mathbb{M}_d(R)) = \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix}.$$

In this paper, we completely solve the problem of computing  $S_k(R)$  for any finite commutative unital ring. To do so, we first recall some well-known ring-theoretic facts. If  $R$  is a finite commutative unital ring with  $\text{char}(R) = n = p_1^{t_1} \cdots p_l^{t_l}$ , then we have a decomposition of  $R$  as a direct product of rings

$$(1) \quad R \cong R_1 \times \cdots \times R_l,$$

where  $\text{char}(R_i) = p_i^{t_i}$ . Moreover, for every  $i \in \{1, \dots, l\}$ , the ring  $R_i$  can be seen as a  $\mathbb{Z}/p_i^{t_i}\mathbb{Z}$ -module and hence it can be decomposed as a direct sum of cyclic modules

$$(2) \quad R_i \cong R_{i,1} \oplus \cdots \oplus R_{i,m_i},$$

with  $\text{ann}(R_{i,j}) = (p_i^{t_j})$  and  $1 \leq t_j \leq t_i$ .

## 2. THE PRIME-POWER CHARACTERISTIC CASE

Decomposition (1) above implies that, in order to get a general result, we can restrict ourselves to the prime-power characteristic case. Hence, throughout this section  $R$  will be a finite commutative unital ring with  $\text{char}(R) = p^t$ .

Due to decomposition (2),  $R$  is the direct sum of cyclic modules. If  $R$  is itself a cyclic  $\mathbb{Z}/p^t\mathbb{Z}$ -module, then  $R \cong \mathbb{Z}/p^t\mathbb{Z}$  and Proposition 1 ii) applies to obtain that  $S_k(R) = -p^{t-1}$  if  $p-1 \mid k$  and  $S_k(R) = 0$  otherwise. Thus, we will focus on the non-cyclic case.

First of all, we will prove that if  $t > 1$ ; i.e., if the characteristic is a prime-power but not a prime then  $S_k(R) = 0$ .

**Proposition 3.** *Let  $R$  be a finite commutative unital ring such that  $\text{char}(R) = p^t$  with  $t > 1$ . If  $R$  is not a cyclic  $\mathbb{Z}/p^t\mathbb{Z}$ -module, then  $S_k(R) = 0$  for every  $k \geq 1$ .*

*Proof.* Due to decomposition (2) we have that  $R \cong R_1 \oplus \cdots \oplus R_m$  with  $m \geq 2$ ,  $R_i$  cyclic and  $\text{ann}(R_i) = (p^{t_i})$  with  $1 \leq t_i \leq t$ .

Hence, if we denote by  $x_i$  a generator of  $R_i$ , then every element of  $R$  can be uniquely written in the form  $a_1x_1 + \dots + a_mx_m$  with  $a_i \in \{0, \dots, p^{t_i} - 1\}$  for every  $i \in \{1, \dots, m\}$ . Thus,

$$S_k(R) = \sum_{a_i=0}^{p^{t_i}-1} (a_1x_1 + \dots + a_mx_m)^k = \sum_{s=0}^k \sum_{a_i=0}^{p^{t_i}-1} \binom{k}{s} (a_1x_1)^s (a_2x_2 + \dots + a_mx_m)^{k-s}$$

and we will proceed inductively.

First of all, assume that  $m = 2$ . In this case,

$$S_k(R) = \sum_{s=0}^k \binom{k}{s} \sum_{a_1=0}^{p^{t_1}-1} \sum_{a_2=0}^{p^{t_2}-1} (a_1x_1)^s (a_2x_2)^{k-s}$$

and note that either  $t_1 \geq 2$  or  $t_2 \geq 2$ , for if  $t_1, t_2 < 2$  then  $t = 1$  which is not possible.

For every  $s \in \{0, \dots, k\}$ , denote by  $A(s) := \sum_{a_1=0}^{p^{t_1}-1} \sum_{a_2=0}^{p^{t_2}-1} (a_1x_1)^s (a_2x_2)^{k-s}$ . Now,

since  $p^{t_i}x_i = 0$  we have that

$$\begin{aligned} A(0) &= \sum_{a_1=0}^{p^{t_1}-1} \sum_{a_2=0}^{p^{t_2}-1} (a_2x_2)^k = p^{t_2} \sum_{a_2=0}^{p^{t_2}-1} (a_2x_2)^k = 0, \\ A(k) &= \sum_{a_1=0}^{p^{t_1}-1} \sum_{a_2=0}^{p^{t_2}-1} (a_1x_1)^k = p^{t_1} \sum_{a_1=0}^{p^{t_1}-1} (a_1x_1)^k = 0. \end{aligned}$$

On the other hand, if  $0 < s < k$ ,

$$A(s) = \sum_{a_1=0}^{p^{t_1}-1} (a_1x_1)^s \sum_{a_2=0}^{p^{t_2}-1} (a_2x_2)^{k-s}$$

and due to Proposition 1 ii) we have that  $\sum_{a_1=0}^{p^{t_1}-1} (a_1x_1)^s$  is either 0 or  $-p^{t_1-1}x_1^s$  and

also that  $\sum_{a_2=0}^{p^{t_2}-1} (a_2x_2)^{k-s}$  is either 0 or  $-p^{t_2-1}x_2^{k-s}$ . Consequently, it follows that

either  $A(s) = 0$  or  $A(s) = p^{t_1+t_2-2}x_1^s x_2^{k-s}$  but in this latter case, since either  $t_1 \geq 2$  or  $t_2 \geq 2$ , it also follows that  $A(s) = 0$  as claimed.

Now, if  $m > 2$ ,

$$S_k(R) = \sum_{s=0}^k \binom{k}{s} \sum_{a_1=0}^{p^{t_1}-1} (a_1x_1)^s \sum_{\substack{a_i=0 \\ i \neq 1}}^{p^{t_i}-1} (a_2x_2 + \dots + a_mx_m)^{k-s}$$

and for every  $0 \leq s \leq k$  at least one of the summatories appearing in the latter expression is 0 by induction hypothesis.  $\square$

The following series of technical lemmata will be useful when we consider the case  $t = 1$  in the sequel. In what follows  $\mathbb{F}_q$  will denote the field with  $q$  elements.

**Lemma 1.** *Let  $R$  be a finite commutative unital  $\mathbb{F}_q$ -algebra with  $q > 2$  such that there exists  $x \in R - \{0\}$  with  $x^2 = 0$ . Then,  $S_k(R) = 0$  for every  $k$ .*

*Proof.* Given  $x \in R - \{0\}$  with  $x^2 = 0$  we can decompose  $R$  as the direct sum of vector subspaces  $R = \langle x \rangle \oplus \bar{R}$ . Thus,

$$\begin{aligned} S_k(R) &= \sum_{a \in \mathbb{F}_q} \sum_{t \in \bar{R}} (ax + t)^k = \sum_{a \in \mathbb{F}_q} \sum_{t \in \bar{R}} (t^k + kt^{k-1}ax) = \\ &= q \sum_{t \in \bar{R}} t^k + \sum_{a \in \mathbb{F}_q} a \sum_{t \in \bar{R}} kt^{k-1}x = 0, \end{aligned}$$

because, for  $q > 2$ , it holds that  $\sum_{a \in \mathbb{F}_q} a = 0$  due to Proposition 1 i).  $\square$

**Lemma 2.** *Let  $R$  be a finite commutative unital  $\mathbb{F}_q$ -algebra such that there exist a free family  $\{x, y\}$  with  $xy = 0$ . Then,  $S_k(R) = 0$  for every  $k$ .*

*Proof.* Given a free family  $\{x, y\}$  with  $xy = 0$  we can decompose  $R$  as the direct sum of vector subspaces  $R = \langle x \rangle \oplus \langle y \rangle \oplus \bar{R}$ . Thus,

$$\begin{aligned} S_k(R) &= \sum_{a \in \mathbb{F}_q} \sum_{b \in \mathbb{F}_q} \sum_{t \in \bar{R}} (ax + by + t)^k = \\ &= \sum_{a \in \mathbb{F}_q} \sum_{b \in \mathbb{F}_q} \sum_{t \in \bar{R}} \left( t^k + \sum_{s=1}^k \binom{k}{s} (a^s x^s + b^s y^s) t^{k-s} \right) = \\ &= q^2 \sum_{t \in \bar{R}} t^k + q \sum_{a \in \mathbb{F}_q} \sum_{t \in \bar{R}} \sum_{s=1}^k \binom{k}{s} a^s x^s t^{k-s} + q \sum_{b \in \mathbb{F}_q} \sum_{t \in \bar{R}} \sum_{s=1}^k \binom{k}{s} b^s y^s t^{k-s} = 0 \end{aligned}$$

as claimed.  $\square$

**Lemma 3.** *Let  $R \cong (\mathbb{Z}/2\mathbb{Z})[x]/(x^2)$  and let  $u$  be the only non-zero idempotent of  $R$ . Then,  $S_k(R) = u$  if  $k > 1$  is odd and  $S_k(R) = 0$  otherwise.*

*Proof.* In this situation,  $R = \{0, 1, u, 1 + u\}$  and since  $\text{char}(R) = 2$ , we have that

$$S_k(R) = 0^k + 1^k + u^k + (1 + u)^k = ku$$

and the result follows.  $\square$

Now, we are in the conditions to prove the main result of this section.

**Theorem 1.** *Let  $R$  be a finite commutative unital ring of prime-power characteristic. Then,  $S_k(R) \neq 0$  if and only if one of the following conditions hold.*

- i)  $|R| - 1 \mid k$  and  $R$  is a field.
- ii)  $R \cong \mathbb{Z}/p^s\mathbb{Z}$  and  $p - 1 \mid k$ .
- iii)  $R \cong (\mathbb{Z}/2\mathbb{Z})[x]/(x^2)$  and  $k > 1$  is odd.

*Proof.* If condition i) holds, then  $S_k(R) \neq 0$  due to Proposition 1 i). If condition ii) holds, then  $S_k(R) \neq 0$  due to Proposition 1 ii). If condition iii) holds, then  $S_k(R) \neq 0$  due to Lemma 3.

Conversely, assume that  $S_k(R) \neq 0$ . Proposition 3 implies that  $R$  must be cyclic or it must have prime characteristic. If it is cyclic, then Proposition 1 i) or ii) applies (depending on whether  $R$  is a field or not) and condition i) or ii) holds, respectively. If  $R$  is not cyclic and has prime characteristic, Lemma 2 implies that  $R$  cannot contain two different zero-divisors. Consequently, not being a field,  $R$  must contain idempotents but in this case Lemma 1 implies that  $\text{char}(R) = 2$ . But

all the previous restrictions lead to  $R \cong (\mathbb{Z}/2\mathbb{Z})[x]/(x^2)$  so Lemma 3 applies and the result follows.  $\square$

As a consequence, we obtain the following corollary that gives a characterization of finite fields in terms of power sums. The proof is straightforward and we omit.

**Corollary 1.** *Let  $R$  be a finite commutative unital ring such that  $|R|$  is a prime-power. Then, the following are equivalent.*

- i)  $R$  is a field.
- ii)  $S_k(R) = 0$  or  $S_k(R) = -1$  for every  $k \geq 1$ .
- iii)  $S_k(R) = -1$  for  $k = |R| - 1$ .
- iv) There exists  $k \geq 1$  such that  $S_k(R) = -1$ .

**Remark.** Corollary 1 provides an elementary (although inefficient) algorithm to determine if a polynomial with integer coefficients is irreducible over  $\mathbb{Z}/p\mathbb{Z}$ . Its computational complexity is exponential, thus it is worse than the fast already known algorithms for the factorization of polynomials [8]. Moreover, it also determines if an ideal in  $\mathbb{Z}/p\mathbb{Z}[x_1, \dots, x_m]$  is maximal.

For instance, let us consider  $I = (1 + x^2 + y^2, -1 - x + y^2) \triangleleft \mathbb{Z}/3\mathbb{Z}[x, y]$ . We will prove that this ideal is maximal. To do so, we compute the sum

$$\sum_{0 \leq a, b, c, d < 3} (a + bx + cy + dxy)^{80},$$

doing repeatedly the substitutions  $x^n \rightarrow x^{n-2}(2 + 2y^2)$  and  $y^n \rightarrow y^{n-2}(1 + x)$  when necessary until we arrive to an expression of the form  $A + Bx + Cy + Dxy$ . The ideal  $I$  is maximal if and only if  $A \equiv 2 \pmod{3}$  and  $B \equiv C \equiv D \equiv 0 \pmod{3}$ , which is the case.

### 3. THE GENERAL CASE

In the previous section we have focused on the case when the characteristic of the ring is a prime-power. Now, we will focus on the general case. Let  $R$  be a finite commutative unital ring and assume that  $|R| = p_1^{s_1} \cdots p_l^{s_l}$ . This implies that  $\text{char}(R) = p_1^{t_1} \cdots p_l^{t_l}$  with  $1 \leq t_i \leq s_i$  for every  $i$ . Note that  $t_i = s_i$  if and only if  $R_i$  is isomorphic to  $\mathbb{Z}/p_i^{s_i}$ . In this situation, we define rings  $R_i = R/p_i^{t_i}R$  for every  $i \in \{1, \dots, l\}$ . Note that  $\text{char}(R_i) = p_i^{t_i}$  and, moreover,  $R \cong R_1 \times \cdots \times R_l$  is precisely the decomposition given in (1).

In this setting, given  $k \geq 1$ , let us define the sets

$$\mathcal{P}_k(R) := \{p_i : R_i \text{ is a field and } p_i^{s_i} - 1 \mid k\},$$

$$\overline{\mathcal{P}}_k(R) := \{p_i : R_i \text{ is isomorphic to } \mathbb{Z}/p_i^{s_i}\mathbb{Z} \text{ with } s_i > 1 \text{ and } p_i - 1 \mid k\}.$$

The following lemma is straightforward.

**Lemma 4.** *Let  $R_1$  and  $R_2$  be finite commutative unital ring and let  $R = R_1 \times R_2$  be its direct sum. Then,*

$$S_k(R) = (|R_2|S_k(R_1), |R_1|S_k(R_2)).$$

Now, we are in the condition to prove the main result of the paper.

**Theorem 2.** *Let  $R$  be a finite commutative unital ring with  $|R| = p_1^{s_1} \cdots p_l^{s_l}$  and let  $k \geq 1$  be an integer. Then, with the previous notation*

i) If  $k$  is even, then

$$S_k(R) = - \left( \sum_{p_i \in \mathcal{P}_k} \frac{|R|}{p_i^{s_i}} + \sum_{p_i \in \overline{\mathcal{P}}_k} \frac{|R|}{p_i} \right).$$

ii) If  $k > 1$  is odd and  $2 \in \mathcal{P}_k$ , then

$$S_k(R) = -\frac{|R|}{2^{\nu_2(|R|)}}.$$

iii) If  $k > 1$  is odd and  $2 \in \overline{\mathcal{P}}_k$ , then

$$S_k(R) = -\frac{|R|}{2}.$$

iv) If  $k > 1$  is odd and  $R_i \cong (\mathbb{Z}/2\mathbb{Z})[x]/(x^2)$  for some  $i$ , then

$$S_k(R) = u,$$

where  $u$  is the only non-zero nilpotent element of  $R$  such that  $2u = 0$ .

v) If  $k = 1$  and  $R_i \cong \mathbb{Z}/2\mathbb{Z}$  for some  $i$ , then

$$S_k(R) = -\frac{|R|}{2}.$$

vi) In any other case,  $S_k(R) = 0$ .

*Proof.* First of all, observe that Lemma 4 implies that

$$S_k(R) = \left( \frac{|R|}{p_1^{s_1}} S_k(R_1), \dots, \frac{|R|}{p_l^{s_l}} S_k(R_l) \right).$$

Now,

- i) If  $k$  is even, Theorem 1 implies that  $S_k(R_i) = 0$  unless  $R_i$  is a field with  $|R_i| - 1 \mid k$  or  $R_i \cong \mathbb{Z}/p_i^{s_i}\mathbb{Z}$  with  $p_i - 1 \mid k$  (recall that in this case  $\text{char}(R_i) = |R_i|$ ). Due to Proposition 1 i) and ii), in the first case  $S_k(R_i) = -1$  while in the second case  $S_k(R_i) = -p_i^{s_i-1}$ . Hence, the result follows.
- ii) If  $k > 1$  is odd and  $2 \in \mathcal{P}_k$ , we can assume without loss of generality that  $p_1 = 2$ . Then, Theorem 1 implies that  $S_k(R_i) = 0$  for every  $i \geq 2$  and the result follows from Proposition 1 i).
- iii) It is enough to reason like in ii) but the result follows from Proposition 1 ii).
- iv) Again, the same idea as in ii) and iii) but the claim follows from Lemma 3.
- v) The same as in ii), iii) and iv). Note that in this case  $2 \in \mathcal{P}_k$  and we can apply either Proposition 1 i) or ii).
- vi) Theorem 1 states that the only cases in which  $S_k(R_i) \neq 0$  for some  $i$  are precisely the previous ones.

□

Given a finite commutative unital ring  $R$ , let  $\mathbf{i} : \mathbb{Z} \longrightarrow R$  be the unique ring homomorphism defined by  $\mathbf{i}(1) = 1$ . The previous result clearly implies that the power sum  $S_k(R)$  is an element of  $\text{Im}(\mathbf{i})$  unless  $R \cong \mathbb{Z}/2\mathbb{Z}[x]/(x^2) \times S$  with  $k > 1$  odd and  $|S|$  odd.

**Corollary 2.** *If  $k > 1$  is odd and  $R$  contains a unique non-zero nilpotent element  $u$  such that  $2u = 0$ , then  $S_k(R) = u$ . Otherwise,  $S_k(R) \in \mathbf{i}(\mathbb{Z})$ .*

Now, we characterize those finite commutative unital rings such that the power sum  $S_k(R)$  is a unit.

**Corollary 3.** *Let  $R$  be a finite commutative unital ring and let  $k \geq 1$  be an integer. Then,  $S_k(R)$  is a unit if and only if the following conditions hold:*

- i) *There exist fields  $F_1, \dots, F_l$  such that  $R \cong F_1 \times \dots \times F_l$ .*
- ii)  *$\text{char}(F_i) \neq \text{char}(F_j)$  for every  $i \neq j$ .*
- iii)  *$(|F_i| - 1) \mid k$  for every  $1 \leq i \leq l$ .*

*Proof.* Let  $R$  be a finite commutative unital ring. We know that  $R \cong R_1 \times \dots \times R_l$  with  $R_i$  rings with coprime prime-power characteristic. Due to Lemma 4 it is clear that  $S_k(R)$  is a unit in  $R$  if and only if  $S_k(R_i)$  is a unit in  $R_i$  for every  $i$ . But by Theorem 1 and Proposition 1, this happens if and only if conditions i), ii) and iii) hold.  $\square$

From the previous results the question of determining those finite commutative unital rings  $R$  such that  $S_{|R|}(R) = 1$  naturally arises. This question generalizes the problem of determining the integers  $n$  for which  $\sum_{i=1}^n i^n \equiv 1 \pmod{n}$ . This latter problem was solved in [7, Proposition 1] where it was proved that 1, 2, 6, 42 and 1806 are the only possibilities.

**Theorem 3.** *Let  $R$  be a finite commutative unital ring. Then,  $S_{|R|}(R) = 1$  if and only if the following conditions hold:*

- i)  *$R \cong \mathbb{F}_{p_1^{s_1}} \times \dots \times \mathbb{F}_{p_l^{s_l}}$  with  $p_i \neq p_j$  for every  $i \neq j$ .*
- ii)  *$p_i^{s_i} - 1 \mid |R|$  for every  $1 \leq i \leq s$ .*
- iii)  *$|R| \equiv -p^{s_i} \pmod{p^{s_i+1}}$  for every  $1 \leq i \leq l$ .*

*Proof.* If  $S_{|R|}(R) = 1$ , in particular  $S_k(R)$  is a unit so Corollary 3 applies to give conditions i) and ii). Moreover, using Lemma 4  $S_k(R) = 1$  if and only if  $\frac{|R|}{p_i^{s_i}} S_k(\mathbb{F}_{p_i^{s_i}}) = 1$  in  $\mathbb{F}_{p_i^{s_i}}$ . Since  $S_k(\mathbb{F}_{p_i^{s_i}}) = -1$  due to condition ii) and Proposition 1, condition iii) easily follows.

Conversely, if conditions i), ii) and iii) hold, it is enough to apply Theorem 1 and Proposition 1 as usual to get the result.  $\square$

The following easy corollary relates the previous theorem with [7, Proposition 1].

**Corollary 4.** *Let  $R$  be a finite commutative unital ring such that  $|R|$  is square-free and  $S_{|R|}(R) = 1$ . Then,  $R$  is isomorphic to one of the following rings: the Zero Ring,  $\mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/6\mathbb{Z}$ ,  $\mathbb{Z}/42\mathbb{Z}$  or  $\mathbb{Z}/1806\mathbb{Z}$ .*

*Proof.* Theorem 3 above implies that  $R \cong \mathbb{Z}/n\mathbb{Z}$  for some square-free integer  $n$ . Then,  $S_k(R) = \sum_{i=1}^n i^n$  and it is enough to apply [7, Proposition 1] to get the result.  $\square$

In addition to the aforementioned rings, there is only one more finite commutative unital ring  $R$  with order smaller than  $10^7$  satisfying  $S_{|R|}(R) = 1$ . Namely,

$$\mathbb{F}_{16} \times \mathbb{F}_9 \times \mathbb{F}_5.$$

There are not many rings  $R$  with  $S_{|R|}(R) = -1$  either. The following result, whose proof is identical to that of Theorem 3 (and hence we omit) characterizes them.

**Theorem 4.** *Let  $R$  be a finite commutative unital ring. Then,  $S_{|R|}(R) = -1$  if and only if the following conditions hold:*

- i)  $R \cong \mathbb{F}_{p_1^{s_1}} \times \cdots \times \mathbb{F}_{p_l^{s_l}}$  with  $p_i \neq p_j$  for every  $i \neq j$ .
- ii)  $p_i^{s_i} - 1 \mid |R|$  for every  $1 \leq i \leq l$ .
- iii)  $|R| \equiv p^{s_i} \pmod{p^{s_i+1}}$  for every  $1 \leq i \leq l$ .

We have only been able to find 5 rings with this property: the Zero Ring,  $\mathbb{F}_2$ ,  $\mathbb{F}_4 \times \mathbb{F}_3$ ,  $\mathbb{F}_{16} \times \mathbb{F}_{81} \times \mathbb{F}_{25}$ ,  $\mathbb{F}_{16} \times \mathbb{F}_{81} \times \mathbb{F}_5 \times \mathbb{F}_{11}$ . The orders of the non-zero cases are: 2, 12, 32400 and 71280.

#### 4. POWER SUMS OVER $\mathbb{Z}/n\mathbb{Z}[x]/(f(x))$

As an application of the previous results, we are interested in computing the power sum  $S_k(\mathbb{Z}/n\mathbb{Z}[x]/(f(x)))$ , where  $f(x)$  is a monic polynomial. When  $\deg f = 1$ , the result is straightforward because  $\mathbb{Z}/n\mathbb{Z}[x]/(f(x)) \cong \mathbb{Z}/n\mathbb{Z}$  and Proposition 1 ii) applies.

In order to study the case when  $\deg f > 1$  we will first focus on the quadratic case.

##### 4.1. Power sums over $\mathbb{Z}/n\mathbb{Z}[x]/(x^2 + bx + c)$ .

Before we proceed, let us introduce some notation. Given any positive integer  $n$  and integers  $b, c$  we define

$$R_n^{b,c} := \mathbb{Z}/n\mathbb{Z}[x]/(x^2 + bx + c).$$

As usual, to compute the value of  $S_k(R_n^{b,c})$  we will first focus on the case when  $n$  is a prime power.

**Proposition 4.** *Let  $k \geq 1$  be and integer.*

- i) *If  $s$  is a positive integer,*

$$S_k(R_{2^s}^{b,c}) = \begin{cases} 1, & \text{if } s = 1, b \text{ and } c \text{ are odd and } 3 \mid k; \\ 1 + x, & \text{if } s = 1, b \text{ is even, } c \text{ is odd and } k > 1 \text{ is odd;} \\ x, & \text{if } s = 1, b \text{ and } c \text{ are even and } k > 1 \text{ is odd;} \\ 0 & \text{otherwise.} \end{cases}$$

- ii) *If  $p$  is an odd prime and  $s$  is a positive integer,*

$$S_k(R_{p^s}^{b,c}) = \begin{cases} -1, & \text{if } s = 1, p^2 - 1 \mid k \text{ and } b^2 - 4c \text{ is not a square mod. } p; \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* i) First of all, if  $s > 1$  then  $\text{char}(R_{2^s}^{b,c}) \geq 4$  and we can apply Proposition 3 to obtain that  $S_k(R_{2^s}^{b,c}) = 0$  for every  $k$  in this case.

If  $s = 1$  and both  $b$  and  $c$  are even, then  $R_{2^s}^{b,c} = \mathbb{Z}/2\mathbb{Z}/(x^2)$  and by Lemma 3 it follows that  $S_k(R_{2^s}^{b,c}) = x$  if  $k > 1$  is odd and  $S_k(R_{2^s}^{b,c}) = 0$  otherwise.

If  $s = 1$ ,  $b$  is even and  $c$  is odd, then  $R_{2^s}^{b,c} = \mathbb{Z}/2\mathbb{Z}/(x^2 + 1)$  and by Lemma 3 it follows that  $S_k(R_{2^s}^{b,c}) = 1 + x$  if  $k > 1$  is odd (note that  $1 + x$  is the only non-zero nilpotent element) and  $S_k(R_{2^s}^{b,c}) = 0$  otherwise.



If  $s = 1$ ,  $b$  is odd and  $c$  is even, then  $R_{2^s}^{b,c} = \mathbb{Z}/2\mathbb{Z}/(x^2 + x)$ . Since  $0 = x^2 + x = x(x+1)$ , we can apply Lemma 2 to obtain that  $S_k(R_{2^s}^{b,c}) = 0$  for every  $k$  in this case.

Finally, if both  $b$  and  $c$  are odd, then  $R_{2^s}^{b,c} = \mathbb{Z}/2\mathbb{Z}/(x^2 + x + 1) \cong \mathbb{F}_4$  because  $x^2 + x + 1$  is irreducible. Hence, we apply Proposition 1 i) to obtain that  $S_k(R_{2^s}^{b,c}) = -1 = 1$  if  $3 \mid k$  and  $S_k(R_{2^s}^{b,c}) = 0$  otherwise.

- ii) First of all, if  $s > 1$  then  $\text{char}(R_{p^s}^{b,c}) \geq p^2$  and we can apply Proposition 3 to obtain that  $S_k(R_{p^s}^{b,c}) = 0$  for every  $k$  in this case.

If  $s = 1$ , observe that  $x^2 + bx + c$  is reducible if and only if  $b^2 - 4c$  is a quadratic residue modulo  $p$ . Now, if  $x^2 + bx + c$  is reducible we can apply Lemma 1 or Lemma 2 to obtain that  $S_k(R_{p^s}^{b,c}) = 0$  for every  $k$ . Finally, if  $x^2 + bx + c$  is irreducible then  $R_{p^s}^{b,c} \cong \mathbb{F}_{p^2}$  and Proposition 1 i) ends the proof.  $\square$

With this proposition, we can prove the general result.

**Theorem 5.** *Let  $n$  be any positive integer. Given integers  $k \geq 1$ ,  $b$  and  $c$  we define the following set:*

$$\mathcal{P}^{b,c}(k, n) := \{\text{prime } p : p \mid n, p^2 - 1 \mid k, b^2 - 4c \text{ is not a quadratic residue modulo } p\}.$$

*Then:*

$$S_k(R_n^{b,c}) = \begin{cases} \frac{n}{2}, & \text{if } b \text{ and } c \text{ are odd, } 3 \mid k \text{ and } 2 \parallel n; \\ \frac{n}{2}(1+x), & \text{if } b \text{ is even, } c \text{ is odd, } k > 1 \text{ is odd, and } 2 \parallel n; \\ \frac{n}{2}x, & \text{if } b \text{ and } c \text{ are even, } k > 1 \text{ is odd and } 2 \parallel n; \\ - \sum_{p \in \mathcal{P}^{b,c}(k,n)} \frac{n^2}{p^2}, & \text{otherwise.} \end{cases}$$

*Proof.* Observe that for coprime  $n_1$  and  $n_2$  we have that  $R_{n_1 n_2}^{b,c} \cong R_{n_1}^{b,c} \times R_{n_2}^{b,c}$ . Thus, it suffices to apply Proposition 4 above.  $\square$

As an interesting consequence of this result, we can compute the power sum over the rings  $\mathbb{Z}/n\mathbb{Z}[\sqrt{D}]$  for a square-free integer  $D$ .

**Corollary 5.** *Let  $k, n \geq 1$  be integers and let  $D$  be a square-free integer. Consider the set*

$$\mathcal{P}(k, n) := \{\text{prime } p : p \mid n, p^2 - 1 \mid k, D \text{ is not a quadratic residue modulo } p\}.$$

*Then,*

$$S_k(\mathbb{Z}_n[\sqrt{D}]) = \begin{cases} \frac{n}{2}(1 + \sqrt{D}), & \text{if } k > 1 \text{ is odd and } 2 \parallel n; \\ - \sum_{p \in \mathcal{P}(k,n)} \frac{n^2}{p^2}, & \text{otherwise.} \end{cases}$$

*Proof.* Just take  $f(x) = x^2 - D$  and apply Theorem 5.  $\square$

**Remark.** If we consider the case  $D = -1$ , the previous corollary immediately gives Proposition 1 iii), which was proved in [3] using different, more direct, techniques.

#### 4.2. Power sums over $\mathbb{Z}/n\mathbb{Z}[x]/(f(x))$ with $\deg f > 2$ .

Now, we focus on the case when the degree of the considered polynomial is greater than 2. The involved ideas are quite similar to those previously used. We introduce the following notation:

$$R_n^f := \mathbb{Z}/n\mathbb{Z}[x]/(f(x)).$$

**Theorem 6.** *Let  $f(x)$  be monic polynomial with integer coefficients such that  $\deg f > 2$  and let  $k, n \geq 1$  be integers. Consider the set*

$$\mathcal{P}^f(k, n) := \{\text{prime } p : p \mid n, p^{\deg f} - 1 \mid k, f(x) \text{ is irreducible modulo } n\}.$$

Then,

$$S_k(R_n^f) \equiv - \sum_{p \in \mathcal{P}^f(k, n)} \frac{n^{\deg f}}{p^{\deg f}}.$$

*Proof.* Let  $n = p_1^{s_1} \dots p_l^{s_l}$ . Then, as usual

$$R_n^f \cong R_{p_1^{s_1}}^f \times \dots \times R_{p_l^{s_l}}^f$$

and we can apply Lemma 4.

First of all, note that  $S_k(R_{p_i^{s_i}}^f) = -1$  if  $p_i \in \mathcal{P}(n, k)$  and  $S_k(R_{p_i^{s_i}}^f) = 0$  otherwise. Since  $|R_n^f| = n^{\deg f}$ , the result follows.  $\square$

### 5. FUTURE PERSPECTIVES

**5.1. Power sums over non-commutative rings.** A natural sequel for this work would be to focus on the computation of  $S_k(R)$  for more general rings. In particular, the non-commutative case seems interesting and we can pose the following question.

**Question 1.** Is there any finite non-commutative ring  $R$  with odd characteristic such that  $S_k(R) \neq 0$  for some  $k$ ?

This question is nontrivial and it is enough to restrict it to prime characteristic rings. Moreover, we have a lower bound for the cardinality of a candidate to answer Question 1 in the affirmative.

**Proposition 5.** *Let  $R$  be a finite non-commutative unital ring with odd characteristic. If  $S_k(R) \neq 0$  for some  $k \geq 1$ , then  $|R| \geq 81$ .*

*Proof.* A finite non-commutative unital ring with prime-power characteristic must have cardinality  $p^s$  for some prime  $p$  and  $s > 2$ . Thus,  $|R| = p^s$  with  $s > 2$ . Now, if  $|R| = p^3$  we have that

$$R \cong \mathbb{Z}/p\mathbb{Z} \langle x, y \rangle / (x^2 = 0, y^2 = 0, xy = x, yx = 0)$$

because, up to isomorphism, there exists just one finite non-commutative unital ring with  $p^3$  elements. Since, in this case it is easy to see that  $S_k(R) = 0$  the result follows.  $\square$

**5.2. Finite commutative unital rings such that  $S_{|R|}(R) = \pm 1$ .** At the end of Section 3, we have given the characterizations of finite commutative unital rings satisfying  $S_{|R|}(R) = \pm 1$ . Those characterizations allowed us to find, by computational means, rings with these properties. Hence, it arises the question of finding some strategies to search for these rings and even to find out if there is a finite number of them (as in the case of square-free  $|R|$ )

**5.3. Rings such that  $S_{|R|-1}(R) = -1$ . Generalized Giuga's conjecture.** If  $R$  is a field  $S_{|R|-1}(R) = -1$ . The converse is true (see Corollary 1) if we restrict to rings with prime-power characteristic. This immediately suggests the question about the existence of a ring  $R$  which is not a field and satisfying that  $S_{|R|-1}(R) = -1$ . The following result gives a characterization of such a ring.

**Theorem 7.** *Let  $R$  be a finite commutative unital ring. Then,  $S_{|R|-1}(R) = -1$  if and only if the following conditions hold:*

- i)  $R \cong \mathbb{F}_{p_1^{s_1}} \times \cdots \times \mathbb{F}_{p_l^{s_l}}$  with  $p_i \neq p_j$  for every  $i \neq j$ .
- ii)  $p_i^{s_i} - 1 \mid |R| - 1$  for every  $1 \leq i \leq l$ .
- iii)  $|R| \equiv p^{s_i} \pmod{p^{s_i+1}}$  for every  $1 \leq i \leq l$ .

Condition ii) is satisfied by many integers (by Carmichael numbers, for instance). Nevertheless, we have not been able to find among them any integer satisfying also condition iii). This question is closely related to Giuga's conjecture [5] that states that there are no square-free compound integers satisfying conditions ii) and iii)

above. In other words, Giuga's conjecture states that  $\sum_{i=1}^n i^{n-1} \equiv -1 \pmod{n}$  if and only if  $n$  is prime. Hence, we propose the following generalization of Giuga's conjecture.

**Conjecture 2.** *Let  $R$  be a finite commutative unital ring. Then  $\sum_{r \in R} r^{|R|-1} = -1$  if and only if  $R$  is a field.*

## REFERENCES

- [1] J.V. Brawley, L. Carlitz, J. Levine. Power sums of matrices over a finite field. *Duke Math. J.*, 41:9–24, 1974.
- [2] L. Carlitz. The Staudt-Clausen theorem. *Math. Mag.*, 34:131–146, 1960–1961.
- [3] P. Fortuny, J.M. Grau, A. M. Oller-Marcén. A von Staudt-type result for  $\sum_{z \in \mathbb{Z}_n[i]} z^k$ . *Monatsh. Math.* DOI: 10.1007/s00605-015-0736-5, 2015.
- [4] P. Fortuny, J.M. Grau, A. M. Oller-Marcén, I.F. Rúa On power sums of matrices over a finite commutative ring. arXiv:1505.08132 [math.RA].
- [5] G.Giuga. Su una presumibile proprietà caratteristica dei numeri primi. *Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. (3)*, 14(83):511–528, 1950.
- [6] J.M. Grau, P. Moree, A.M. Oller-Marcén. Solutions of the congruence  $\sum_{k=1}^n k^{f(n)} \equiv 0 \pmod{n}$ . *Math. Nachr.*, DOI: 10.1002/mana.201500057, 2015.
- [7] J.M. Grau, A.M. Oller-Marcén, J. Sondow. On the congruence  $1^m + 2^m + \cdots + m^m \equiv n \pmod{m}$  with  $n \mid m$ . *Monatsh. Math.*, DOI 10.1007/s00605-014-0660-0, 2014.
- [8] E. Kaltofen. Polynomial Factorization 1987–1991. *Springer Lect. Notes Comput. Sci.*, 583: 294–313, 1992.
- [9] P. Moree. On a theorem of Carlitz-von Staudt. *C. R. Math. Rep. Acad. Sci. Canada*, 16(4):166–170, 1994.
- [10] K. G. C. von Staudt. Beweis eines Lehrsatzes die Bernoullischen Zahlen betreffend. *J. Reine Angew. Math.*, 21:372–374, 1840.

DEPARTAMENTO DE MATEMÁTICAS, UNIVERSIDAD DE OVIEDO, AVDA. CALVO SOTELO s/N, 33007 OVIEDO, SPAIN

E-mail address: grau@uniovi.es

CENTRO UNIVERSITARIO DE LA DEFENSA DE ZARAGOZA, CTRA. HUESCA s/N, 50090 ZARAGOZA, SPAIN

E-mail address: oller@unizar.es